"Encrypta: A missão da liga dos robôs" - Um jogo educacional para aprendizagem em cibersegurança

"Encrypta: The robot league mission" - An educational game for cybersecurity learning

Jeanluca Martins de Abreu[1], **Rodrigo Sanches Miani** [1], **Shigueo Nomura**[1]

Faculdade de Computação – Universidade Federal de Uberlândia – Campus Santa Mônica
Av. João Naves de Ávila, 2121 - Santa Mônica, Uberlândia - MG, 38408-100

{jeanluca.abreu, shigueonomura, miani }@ufu.br

Abstract. *It has beeen notorious that cyber attacks have increased tightly due to the large volume of data shared by users on the web. And those users (including young Brazilians) have been targeted by cybercriminals. In this work, the digital game Encrypta was developed to protect teenagers from cyber attacks in the internet. The strategy is to look for ways to educate or train those young gamers, preventing them from becoming victims of those crimes. The Virtual Reality Systems (SRV) development methodology was adopted to implement this proposal. Experimental tests of the developed system showed promising results in relation to the game's usability and teaching capacity.*
Keywords— *digital games, educational game, cybersecurity.*

Resumo. *Notadamente, ataques cibernéticos têm aumentado significantemente por causa do grande volume de dados compartilhados por usuários na web. E esses usuários (incluindo jovens brasileiros) têm sido visados por cibercriminosos. Neste trabalho, o jogo digital Encrypta foi desenvolvido para proteger os adolescentes dos ataques cibernéticos na internet. A estratégia é buscar formas de educar ou treinar esses jovens jogadores, evitando que eles se tornem vítimas desses crimes. A metodologia de desenvolvimento de Sistemas de Realidade Virtual (SRV) foi adotada para a execução desta proposta. Testes experimentais do sistema desenvolvido apresentaram resultados promissores em relação à usabilidade e capacidade de ensino do jogo.*
Palavras-chave— *jogos digitais, jogo educacional, cibersegurança.*

1. Introdução

Segundo dados apresentados pelo Instituto Brasileiro de Geografia e Estatística [IBGE 2023], o Brasil possui uma população de 203 milhões de habitantes. Pesquisas realizadas em 2023 mostram que existem 464 milhões de dispositivos conectados à internet no país, abrangendo dispositivos como computadores, *notebooks*, *tablets* e *smartphones*, totalizando uma média de 2,2 aparelhos por habitante. O estudo estima que até o ano de 2024 haverá em média 1 *smartphone* por habitante no mundo [Meirelles 2022].

A pesquisa ainda aponta que entre pessoas da faixa etária de 16 a 64 anos, os jovens adolescentes entre 16 e 24 anos estão entre o grupo da população brasileira que

passa mais tempo do dia em mídias sociais, tornando-se o maior país do mundo em consumo diário, totalizando cerca de 3:40h de uso ao dia por pessoa. Vale salientar que esses dados não estão ligados ao gasto diário total utilizando dispositivos digitais, que pode ser ainda maior, mas exclusivamente ao uso de mídias sociais que possibilitam interações entre usuários, como, por exemplo, o Facebook, Twitter, Instagram, entre outros.

Os crimes cibernéticos são classificados como crimes que ocorrem em âmbito virtual, onde os infratores usam softwares de computador para encontrar brechas que permitam acessar os dados pessoais dos usuários, danificar seus dispositivos ou até mesmo extorquir as vítimas [Borges e Quinan 2023]. Para garantir a integridade dos usuários perante estas situações, em 2018, a Lei Geral de Proteção de Dados [LGPD 2018] foi criada com o intuito de proteger os direitos e a privacidade dos usuários na internet, tendo como objetivo garantir a segurança das informações pessoais de cada brasileiro.

Com o aumento constante no uso de dispositivos digitais no país, as tentativas de golpes virtuais tendem a aumentar. Dados apresentados pela empresa de cibersegurança Trend Micro revelaram cerca de 7 milhões de tentativas de ataques virtuais no Brasil apenas no primeiro semestre de 2023, classificando-o como o segundo país mais vulnerável a ciberataques do mundo [Micro 2023].

Ignorar meios de alertar adolescentes sobre os perigos virtuais pode colocá-los em sérios riscos, visto que indivíduos que não sabem ou possuem pouco conhecimento sobre os crimes virtuais são geralmente tidos como alvos fáceis por esses criminosos [Ferreira 2023]. É necessário buscar formas de aplicar a educação digital nas instituições de ensino brasileiras, para os estudantes terem capacidade de identificar e lidar com situações de perigo na internet.

Os jogos digitais tornaram-se populares dentro das escolas, sendo utilizados como ferramenta complementar no processo de aprendizagem [da Rocha Côrtes e de Brito Paixão 2023]. Estes possuem a capacidade de propor desafios e prender a atenção dos indivíduos devido à sua natureza lúdica e desafiadora, incentivando e tornando o aprendizado mais divertido.

O jogo digital "Encrypta: A missão da liga dos robôs" foi desenvolvido com o objetivo de educar alunos da educação básica sobre a importância da cibersegurança, abordando temas relacionados aos perigos advindos pela exposição virtual. O jogo apresenta tópicos como o uso de senhas fortes para se proteger de ataques, detecção de e-mails *phishing*, sites e arquivos maliciosos e a prática de se realizar *backups* regulares de dados importantes.

2. Trabalhos Correlatos

Os trabalhos existentes e que serviram de fundamento para o desenvolvimento do projeto e execução desta proposta se encontram apresentados nesta seção. Optou-se por utilizar trabalhos na língua portuguesa com o intuito de fornecer uma visão pautada na realidade educacional do Brasil.

2.1. Aprendendo Segurança da Informação

"Aprendendo Segurança da Informação" é um jogo de RPG, onde o jogador interpreta o funcionário de uma empresa. Ao longo das 5 fases, é possível andar pelo cenário e

interagir com os personagens ali presentes. Em cada uma das fases, ele é apresentado a conceitos importantes de segurança da informação, aprendendo a evitar o uso de pen drives na empresa, os perigos de postar fotos mostrando dados da instituição e a lidar com dados sensíveis, e-mails e sites fraudulentos [Frydman e Bueno 2023].

2.2. *Web* Segura

O jogo digital sério "Web Segura" foi desenvolvido com o intuito de ensinar alunos seniores a compreender e lidar com os perigos presentes na internet. Por meio de quizzes e minijogos interativos, a aplicação aborda questões sobre segurança na internet, como o incentivo ao uso de senhas fortes, formas de detectar sites fraudulentos, notícias falsas e cuidados em compras online [Bernardino et al. 2023].

A Tabela 1 apresenta as principais diferenças entre os jogos apresentados nesta seção. Encrypta visa introduzir novos conteúdos não abordados por esses trabalhos, permite ao jogador selecionar diferentes personagens com jogos temáticos para cada um, e oferece uma espaço para a edição do quiz do jogo destinada aos professores.

Tabela 1. Tabela de Comparação dos Trabalhos Relacionados (Fonte: Elaboração própria)

TRABALHOS	Lúdico	Narrativa	Jogo Educacional	Variedade de jogos	Histórico de jogadores	Seleção de Personagens	Edição de fases do jogo
Web Segura	■		■	■			
Seg. da Informação	■	■	■		■		
Encripta	■	■	■	■		■	■

3. Fundamentação Teórica

Nesta seção, são apresentadas as bases científicas necessárias para o desenvolvimento do projeto.

3.1. Educação Digital

Com o avanço tecnológico, é possível perceber que o consumo de dispositivos digitais é incentivado desde a infância das crianças, tornando-as expostas aos perigos do mundo digital desde os primeiros anos de vida. Através da educação digital, é possível auxiliar esses indivíduos para terem uma relação saudável, respeitosa e segura no âmbito virtual. Por meio dela, é possível apresentar aos usuários formas de identificar e lidar com situações de riscos que são características inerentes à exposição na internet [Teixeira 2023].

3.2. Cibercrime

Com a popularização da internet, o volume de dados sendo compartilhados constantemente tende a ser cada vez maior. Com o aumento desses dados sensíveis sendo compartilhados a todo momento, os cibercriminosos, indivíduos que usam ferramentas de tecnologia da informação para cometer crimes, veem uma oportunidade ideal para praticar delitos virtuais. Os *crackers*, *phishers*, *cyberstalkers*, dentre outros nomes utilizados para determinar os mais variados tipos de praticantes de crimes virtuais, usam diversas abordagens para cometer suas transgressões. Na maioria das vezes, perseguem alvos considerados fáceis, como crianças e adolescentes, com o intuito de praticar crimes como *cyberbullying*, pedofilia e a pornografia infantil [Inagaki 2023].

3.3. Jogos Digitais Educacionais

O uso de jogos digitais como auxílio educacional tem se tornado cada vez mais presente nas instituições de ensino brasileiras. Ao serem comparados com os métodos tradicionais de ensino, os jogos se destacam por serem atividades que promovem a participação ativa dos alunos, os imergindo em um mundo lúdico que possibilita a interação entre os estudantes na sala de aula, provocando uma experiência colaborativa e prazerosa para os participantes [de Oliveira Furtado e Sotil 2024].

Os jogos digitais, quando utilizados no ensino, oferecem várias vantagens aos alunos, tais como a motivação, a interação social em sala de aula e a facilitação da compreensão dos conteúdos apresentados. Eles também promovem a troca de experiências e conhecimentos entre os estudantes [de Oliveira Furtado e Sotil 2024].

É perceptível a influência positiva que os jogos digitais podem trazer quando aplicados no contexto educacional, porém é importante observar que os mesmos devem ser testados para verificar sua usabilidade e eficácia no ensino antes de serem aplicados nas instituições. Além disso, é importante garantir que os educadores responsáveis por realizar a aplicação dos jogos em sala de aula tenham os conhecimentos necessários acerca dos jogos e dos temas, que serão trabalhados para absorver ao máximo as vantagens provenientes desse método de apoio educacional [Schünemann e Garcia 2023].

4. Métodos

Para realizar o desenvolvimento do jogo, foi adotada a metodologia de desenvolvimento de sistemas de realidade virtual (SRV) apresentada nos livros de engenharia de software utilizados como referências na pesquisa [Tori et al. 2006], [Mattioli et al. 2009] e [Sommerville 1997].

Este processo de desenvolvimento compreende as seguintes etapas: Análise de Requisitos, Projeto, Implementação, Avaliação e Implantação.

Análise de Requisitos: Durante a etapa de análise, são levantados todos os requisitos necessários para realizar o desenvolvimento do projeto. Foram definidas as histórias e características dos personagens, esboços de menus, interfaces do usuário e os conteúdos das fases.

Projeto: Na fase de projeto, são definidas as ferramentas a serem utilizadas para implementar os requisitos definidos na etapa anterior. Nessa etapa, foram escolhidas as tecnologias para a criação do jogo. Foi adotada a abordagem de desenvolvimento *web*, utilizando *CSS*, *HTML* e *JS*. Já o *port* para *desktop* foi realizado com o uso do *framework Electron*. Os *sprites* para compor o projeto foram retirados de *assets* disponibilizados gratuitamente pela plataforma de distribuição de jogos independentes [Itch.io 2024]. As músicas e efeitos sonoros escolhidos para a trilha sonora do jogo foram retirados dos repositórios de músicas gratuitas [MixKit 2024] e [Chosic 2024].

Implementação: No estágio de implementação, ocorre o desenvolvimento do projeto utilizando os requisitos e as ferramentas estabelecidas nas etapas anteriores. Foram desenvolvidos os *scripts* referentes às fases, histórias, cenários, *sprites* e demais artefatos do jogo.

Avaliação: Durante a etapa de avaliação, ocorrem testes para validar a eficácia do jogo proposto. Sendo assim, o jogo foi testado e avaliado por um grupo de 10 pessoas.

Os testes foram realizados após a obtenção do termo de consentimento livre e esclarecido dos pais ou responsáveis legais dos participantes.

Implantação: Por fim, na etapa de implantação, deve-se definir o local onde o projeto será implantado para poder ser acessado pelos interessados no futuro. Com isso, o jogo foi hospedado nos servidores da plataforma [Itch.io 2024], onde pode ser acessado e jogado, tanto em sua versão *web* quanto em sua versão *desktop*, disponível para download [Jeanluca Martins de Abreu 2024].

4.1. O Jogo

"Encrypta: A missão da liga dos robôs" é um jogo digital educacional desenvolvido com o intuito de educar adolescentes do ensino básico sobre os perigos virtuais. Durante a jornada, os jogadores conhecem os seis robôs que compõem a liga dos robôs, uma equipe de heróis responsável por manter a ordem na futurista cidade de Encrypta. O jogo apresenta minijogos, quizzes e desafios que abordam tópicos sobre cibersegurança.

- Jogar - possibilita iniciar o jogo;
- Professor - para que o educador possa acessar a área dedicada a ele.

4.2. Níveis do jogo

Ao iniciar, os jogadores descobrem que a cidade de Encrypta foi atacada por um poderoso vírus conhecido como Ômega. Diante dos ataques à Encrypta, a liga dos robôs se une para restaurar a paz. Cada robô possui uma história única, correspondente a uma fase do jogo. Em cada uma dessas fases, os jogadores deverão auxiliar os robôs a combaterem os estragos causados pelo vírus maligno, conforme apresentado na Figura 1.

(a) (b)

Figura 1. a) História de Encrypta b) História do robô Timmy (Fonte: Elaboração própria

História do robô Andy: Andy é o robô responsável por liderar a equipe de heróis. Em sua história, ele foi encurralado pelo vírus Ômega em uma batalha, onde se viu

incapaz de combatê-lo sozinho. Com isso, o robô se escondeu em um cofre de senhas da cidade de Encrypta para se proteger e somente uma senha super forte pode retirar o herói de dentro do artefato. A missão do jogador é controlar Andy pelo cenário, evitando os inimigos enquanto captura esferas de energia que contêm letras, números e caracteres especiais para formar uma senha super forte e retirá-lo de dentro do cofre. Inicialmente, Andy possui três corações de vida. Ao encostar em um inimigo, sua vida é reduzida em um coração, sendo derrotado caso perca todos os corações.

História da robô Rosa: A robô Rosa é a heroína da liga responsável por monitorar os meios de comunicação da cidade, afetados pelo ataque do vírus malicioso. Durante os ataques à Encrypta, ela recebeu uma série de mensagens estranhas em sua caixa de e-mail. Rosa precisa da ajuda do jogador para identificar os e-mails de *phishing*, mensagens fraudulentas que cibercriminosos utilizam visando enganar suas vítimas e roubar seus dados [de Souza e Tanaka 2023]. Os jogadores são apresentados a uma seleção de três e-mails, onde devem identificar e selecionar o e-mail de *phishing*. Caso o jogador selecione e-mails verdadeiros, sua vida será prejudicada, perdendo um ponto de saúde.

Ajudando o robô Andy, os jogadores compreendem a importância de manter senhas fortes para garantir a segurança de seus dados por meio de um jogo de plataforma. Já a história da robô Rosa apresenta um jogo de quebra-cabeça onde é possível compreender a importância de aprender a detectar e eliminar e-mails de *phishing*.

A Figura 2 apresenta as fases do robô Andy e da robô Rosa.

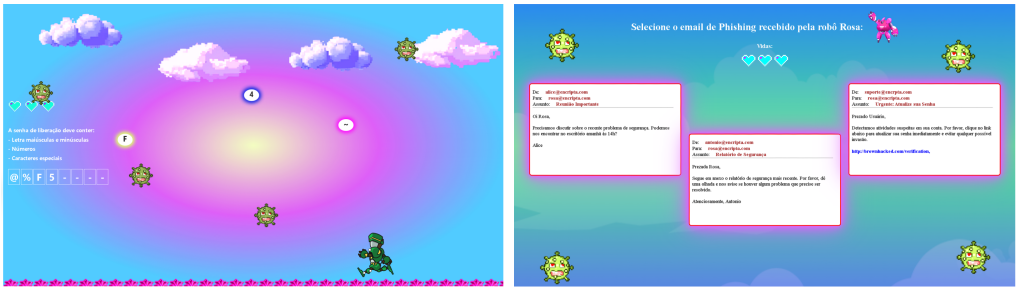


Figura 2. a) Fase do robô Andy b) Fase da robô Rosa (Fonte: Elaboração própria)

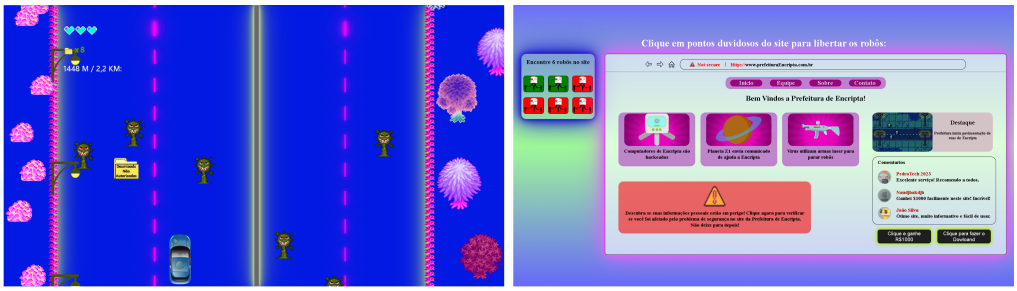
História do robô Turbo: Os documentos mais importantes de Encrypta são guardados no explorador de arquivos, uma enorme pista de corrida cibernética que comporta os arquivos de todos os moradores da cidade. Esta pista é protegida pelo poderoso robô Turbo, que possui a habilidade de se transformar em um carro e percorrê-la em segundos, protegendo-a de todo e qualquer perigo iminente. Durante os ataques à Encrypta, o robô Turbo é responsável por se dirigir ao explorador e verificar se existem pastas infectadas. A missão do jogador é ajudá-lo a percorrer o local, recolhendo as pastas que ainda não foram comprometidas. Durante a fase, os jogadores encontram uma variedade de pastas de arquivos espalhadas pela pista. Eles devem evitar os inimigos e as pastas que possam conter arquivos maliciosos, como pastas de anexos de e-mails desconhecidos e jogos piratas, e coletar as seguras, como pastas de trabalhos escolares, receitas culinárias e documentos importantes para concluir a fase. Ao colidir com inimigos, o jogador perde uma vida, tendo inicialmente três corações disponíveis. Já ao coletar uma pasta maliciosa, o jogador reduz uma unidade na contagem de pastas seguras

coletadas.

História do robô Inspetor: O robô Inspetor é responsável por manter a segurança de todos os sites da cidade de Encrypta, em especial o da prefeitura, sendo este o mais acessado pelos moradores da região. Ele possui a habilidade de se multiplicar para facilitar a inspeção dos sites. Em sua história, ele foi hackeado pelo vírus e várias cópias maliciosas foram espalhadas pelo site da prefeitura. A missão do jogador é encontrar as cópias do robô que estão espalhadas em partes do site que indicam que ele não é seguro, como, por exemplo, *URLs* com *HTTP*, falta de *SSL*, imagens de baixa qualidade, textos com erros textuais, entre outros aspectos que podem auxiliar a detectar sites fraudulentos.

Na história do robô Turbo, os jogadores aprendem a identificar pastas de arquivos maliciosos em um jogo de corrida *top-down*. Já na narrativa do robô Inspetor, eles desenvolvem habilidades para detectar sites fraudulentos em um quebra-cabeça interativo.

Na Figura 3, se verificam as fases do robô Turbo e do robô Inspetor.



(a) (b)

Figura 3. a) Fase do robô Turbo b) Fase do robô Inspetor (Fonte: Elaboração própria)

História do robô Timmy: O robô Timmy é responsável por manter e atualizar os arquivos de *backups* de todos os sistemas da cidade e também dos heróis da liga dos robôs. Em sua história, ele foi procurado por diversos moradores da cidade que temiam a infecção ao acessarem o site da prefeitura para se manterem informados sobre os ataques à Encrypta, em consequência dos ataques sofridos pelo robô Inspetor. Timmy possui arquivos de *backups* de versões anteriores do amigo e parte em uma missão para capturar suas cópias maliciosas, para assim restaurá-las para versões não infectadas. Nesta fase, os jogadores controlam Timmy, onde o objetivo é capturar as cópias infectadas do robô Inspetor e levá-las até a pasta de backup para recuperá-las. Inimigos com padrões de movimentação distintos aparecerão pelo cenário para impedir a progressão do jogador. Assim como nas fases anteriores, três vidas estão disponíveis ao iniciar.

História da robô Charla: Charla é a pesquisadora da liga e é responsável por fazer novas descobertas que auxiliem a cidade e os robôs no combate aos crimes cibernéticos. Em sua mais recente pesquisa, Charla descobre que para derrotar o vírus malicioso, é necessário responder a algumas perguntas sobre cibersegurança que somente os robôs da liga e pessoas que se protegem dos perigos da internet conseguiriam responder. Com isso, a heroína parte para o firewall, um poderoso mecanismo que protege a região e que contém as perguntas que podem salvar a cidade. O desafio do jogador é responder ao quiz descoberto por Charla para restaurar a paz em Encrypta.

Durante a fase do robô Timmy, os jogadores aprendem, por meio de um jogo de plataforma, sobre a importância de armazenar arquivos de backup para recuperação de dados importantes em caso de perda. Já na narrativa de Charla, ao responder ao quiz, os jogadores terão a oportunidade de testar os conhecimentos adquiridos por meio do jogo.

As fases do robô Timmy e da robô Charla são representadas na Figura 4.

(a) (b)

Figura 4. a) Fase do robô Timmy b) Fase da robô Charla (Fonte: Elaboração própria)

4.3. Seção do Professor

Na seção do professor, é possível acessar e editar as questões que compõem o quiz do jogo. Esta área é protegida por senha, concedendo acesso apenas aos professores, como mostra a Figura 5.

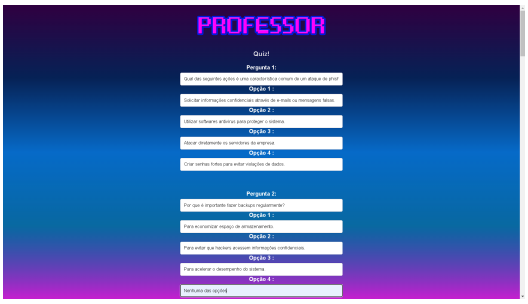


Figura 5. Seção do Professor (Fonte: Elaboração própria)

4.4. Pontos Fortes e Possíveis Melhorias

O jogo aborda tópicos relevantes sobre cibersegurança e sua importância para garantir a segurança online dos usuários. Por meio de desafios interativos, os jogadores lidam com situações que podem ocorrer em seu dia a dia, como o contato direto com e-mails de *phishing*, sites maliciosos, entre outros. Além disso, com base nos quiz disponível no jogo, é possível verificar se os usuários realmente absorveram os conteúdos apresentados.

Por se tratar de um projeto *web*, inicialmente o jogo foi hospedado em um servidor de jogos online e pode ser baixado para ser utilizado em ambiente *desktop*. A aplicação pode ser acessada por dispositivos móveis; no entanto, durante os testes, alguns usuários relataram uma experiência mais satisfatória ao realizar o acesso pelo ambiente *desktop*. Em razão disso, será necessária uma análise mais aprofundada para encontrar as causas que levaram à insatisfação pelos usuários de dispositivos móveis e encontrar uma solução apropriada para o problema.

5. Resultados e Discussão

Esta seção apresenta os testes realizados durante a etapa de avaliação do projeto e os resultados obtidos em cada um deles.

5.1. Teste de Usabilidade e Experiência do Jogador

Com o objetivo de coletar feedback sobre a eficácia do projeto, o jogo foi testado por 10 adolescentes. Os jogadores foram submetidos a um teste contendo 9 perguntas, fundamentadas no modelo MEEGA+, altamente recomendado para a avaliação de jogos digitais educacionais. Este modelo objetiva analisar a aplicabilidade do jogo por meio da avaliação de usabilidade e experiência do jogador [Petri 2019].

Dentre os avaliados, 80% destacaram como ponto forte do jogo os visuais atraentes e interessantes apresentados pelos menus e fases. 90% dos usuários consideraram que o jogo pode alertar de forma simples e clara sobre a importância de lidar com os perigos apresentados pelo ambiente virtual. Além disso, 80% dos entrevistados afirmaram sentir-se favoráveis quando questionados se recomendariam o jogo educacional para outras pessoas. A Figura 6 apresenta os resultados obtidos.

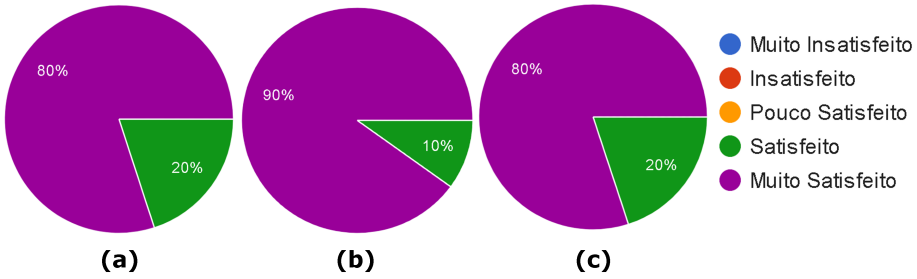


Figura 6. a) O visual do jogo é atraente, interessante? b) Ele pode alertar sobre os perigos da internet? c) Recomendaria o jogo? (Fonte: Elaboração própria)

Os jogadores também apontaram pontos do jogo que merecem atenção. Segundo os entrevistados, pessoas com pouca experiência no uso de computadores podem enfrentar problemas para utilizá-lo, sendo necessária a ajuda de terceiros para conseguir usar a aplicação. Isso se constatou quando 10% dos jogadores responderam estar pouco satisfeitos quando questionados se o jogo era fácil de usar e entender. Os resultados referentes aos pontos de atenção podem ser visualizados na Figura 7.

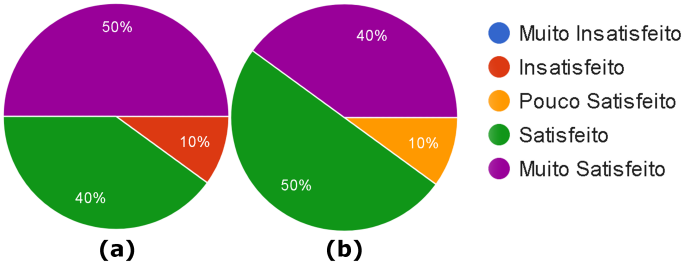


Figura 7. a) O jogo acolhe pessoas de diferentes niveis de experiência com jogos digitais? b) O jogo é fácil de usar/entender? (Fonte: Elaboração própria)

5.2. Teste de Aprendizado

Após realizarem o teste inicial, os mesmos 10 entrevistados responderam às perguntas apresentadas pelo quiz do jogo. As 15 questões de múltipla escolha abordaram situações como identificar e prevenir e-mails de phishing, como reagir ao contato com arquivos e anexos de e-mails desconhecidos, identificação de senhas fortes, práticas seguras de navegação na internet e a importância de *backups* regulares. Conforme a Tabela 2, 3 jogadores cometeram apenas um erro, 1 jogador cometeu 2 erros e 1 jogador cometeu 3 erros. Os demais jogadores conseguiram responder corretamente todas as 15 questões apresentadas pelo teste. Os resultados obtidos indicam que os jogadores absorveram os conteúdos relacionados à cibersegurança abordados, apresentando resultados satisfatórios na resolução das questões do quiz.

Tabela 2. Erros e acertos de cada jogador (Fonte: Elaboração própria)

	Jogadores									
Perguntas	1	2	3	4	5	6	7	8	9	10
1	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
2	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
3	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Erro	Acerto
4	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
5	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
6	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Erro	Acerto	Acerto	Acerto
7	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
8	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
9	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
10	Acerto	Acerto	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
11	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
12	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Erro	Acerto
13	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Erro
14	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
15	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto

6. Conclusão

Considerando o crescente aumento no número de casos de cibercrimes no Brasil, o trabalho proposto foi o desenvolvimento de um jogo digital educacional em que os estudantes são treinados para que não se tornem vítimas de ataques cibernéticos.

Mediante a aplicação do jogo, os voluntários aprenderam a lidar com questões relacionadas à cibersegurança, adquirindo habilidades para detectar e evitar ameaças virtuais.

Testes baseados no modelo MEEGA+ e de aprendizado foram conduzidos com um grupo de voluntários de forma a validar o sistema desenvolvido e sua aplicabilidade.

Resultados promissores foram obtidos a partir dos testes realizados, uma vez que os voluntários mostraram ter absorvido os conteúdos relacionados à cibersegurança, além de destacarem pontos positivos sobre aspectos lúdicos, visuais e interativos do jogo.

Da análise e discussão dos resultados, pode-se concluir que os objetivos propostos neste trabalho foram plenamente atingidos. Como trabalhos futuros, planeja-se adicionar mais tópicos relevantes de cibersegurança ao jogo. Além disso, melhorias deverão ser realizadas na aplicação para o ambiente de dispositivos móveis, visando aperfeiçoar a experiência dos usuários ao acessarem o jogo por meio desses dispositivos.

Referências

[Bernardino et al. 2023] Bernardino, I., Bidarra, J., Baptista, R., e Mamede, H. (2023). Desenvolvimento do jogo sério web segura. *Rotura–Revista de Comunicação, Cultura e Artes*, 3(1):74–101.

[Borges e Quinan 2023] Borges, C. H. M. e Quinan, Y. C. (2023). Crimes cibernéticos: O que são, qual seu real perigo e a importância de dispositivos que garantam a segurança da sociedade.

[Chosic 2024] Chosic (2024). Royalty-free music. Disponivel em: `https://www.chosic.com/`. Acessado em 29 de março de 2024.

[da Rocha Côrtes e de Brito Paixão 2023] da Rocha Côrtes, A. J. M. e de Brito Paixão, E. d. S. (2023). Uso de jogos digitais na educação básica: Análise das abordagens sobre aplicações no contexto escolar nos anos de 2017 a 2020. *Revista Inter-Ação*, 48(3):1013–1024.

[de Oliveira Furtado e Sotil 2024] de Oliveira Furtado, G. e Sotil, J. W. C. (2024). A utilização de jogos educativos digitais no processo de ensino: Vantagens e desafios. *Revista Científica FESA*, 3(14):153–163.

[de Souza e Tanaka 2023] de Souza, L. C. e Tanaka, S. S. (2023). Estudo sobre ataques de phishing e suas técnicas de defesa. *Revista Terra & Cultura: Cadernos de Ensino e Pesquisa*, 39(especial):90–95.

[Ferreira 2023] Ferreira, Y. R. B. (2023). Cibercrimes, cibersegurança e abismo tecnológico nas.

[Frydman e Bueno 2023] Frydman, D. D. e Bueno, N. d. M. (2023). Desenvolvimento de um jogo mobile para ensino de segurança da informação utilizando flutter.

[IBGE 2023] IBGE (2023). Instituto brasileiro de geografia e estatística - censo 2022. Disponivel em: `https://www.ibge.gov.br/`. Acessado em 29 de março de 2024.

[Inagaki 2023] Inagaki, J. Y. M. (2023). Cibercrimes relacionados às crianças e adolescentes.

[Itch.io 2024] Itch.io (2024). Website for indie games and creative resources. Disponivel em: `https://itch.io/`. Acessado em 20 de janeiro de 2024.

[Jeanluca Martins de Abreu 2024] Jeanluca Martins de Abreu (2024). Encrypta: A missão da liga dos robôs - um jogo educacional para aprendizagem em cibersegurança. Disponivel em: `https://jeanluca-a.itch.io/encrypta`. Acessado em 25 de julho de 2024.

[LGPD 2018] LGPD (2018). Lei geral de proteção de dados (lgpd). Disponivel em: `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm`. Lei nº 13.709, de 14 de agosto de 2018.

[Mattioli et al. 2009] Mattioli, F. E., Lamounier Jr, E. A., Cardoso, A., Alves, N., e Muniz, M. (2009). Uma proposta para o desenvolvimento ágil de ambientes virtuais. ***SBC. Anais do WRVA***.

[Meirelles 2022] Meirelles, F. S. (2022). Pesquisa do uso da ti-tecnologia de informação nas empresas. *Fundação Getulio Vargas. https://eaesp. fgv. br/sites/eaesp. fgv. br/files/u68/fgvcia_pes_fi_2022_-_relatorio. pd f.*

[Micro 2023] Micro, T. (2023). Stepping ahead of risk: Trend micro 2023 midyear cybersecurity threat report. Technical report.

[MixKit 2024] MixKit (2024). Royalty-free music and sound effects. Disponivel em: `https://mixkit.co/`. Acessado em 29 de março de 2024.

[Petri 2019] Petri 2019, G. Meega+: A method for the evaluation of the quality of games for computing education.

[Schünemann e Garcia 2023] Schünemann, L. H. A. e Garcia, T. R. (2023). Aplicabilidade de jogos digitais comerciais na educaçao: Uma revisao da literatura. *Anais do XXXIV Simpósio Brasileiro de Informática na Educação*, pages 752–763.

[Sommerville 1997] Sommerville, Ian e Sawyer, P. (1997). Viewpoints: principles, problems and a practical approach to requirements engineering. ***Annals of software engineering***, 3(1):101–130.

[Teixeira 2023] Teixeira, G. C. A. (2023). Educação digital na escola: Cultura de paz e cidadania digital.

[Tori et al. 2006] Tori, R., Kirner, C., e Siscoutto, R. A. (2006). *Fundamentos e tecnologia de realidade virtual e aumentada*. **Editora SBC Porto Alegre**.